PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/JP2004/019124	15.12.2004	17.12.2003

International Patent Classification (IPC) or both national classification and IPC
H04L9/00, G06F1/00

Applicant
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:

European Patent Office - P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tel. +31 70 340 - 2040 Tx: 31 651 epo nl
Fax: +31 70 340 - 3016

Authorized Officer

Holper, G

Telephone No. +31 70 340-2304

ATTACHMENT "F"

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/JP2004/019124

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ in written format

   ☐ in computer readable form

   c. time of filing/furnishing:

   ☐ contained in the international application as filed.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	4-10, 12,13, 18-20, 22, 24-26, 29-33
	No:	Claims	1-3, 11, 14-17, 21, 23, 27, 28, 34-36
Inventive step (IS)	Yes:	Claims	8
	No:	Claims	1-7, 9-36
Industrial applicability (IA)	Yes:	Claims	1-36
	No:	Claims	

2. Citations and explanations

see separate sheet

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY (SEPARATE SHEET)

Re Item V.

1 Reference is made to the following document:

D1: EP-A-1 215 844 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD) 19 June 2002 (2002-06-19)

Claims 1 , 27 and 34 lack clarity (Art. 6 PCT) since the expression "to select ... at least one node encryption key as a selected node encryption key group" is confusing since a single key cannot represent a key group.

Furthermore, the above-mentioned lack of clarity notwithstanding, the subject-matter of claim 1 is not new in the sense of Article 33(2) PCT, and therefore the criteria of Article 33(1) PCT are not met.

D1 discloses (see Fig.2, 4 and 12, the references in parenthesis applying to this document)
a content distribution server (1201) that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses (1202) decrypting the encrypted content and outputting the decrypted content, the content distribution server comprising: a key information storage unit (111) operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method; an encryption key group selection unit (1211) operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group; a content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key (generated by 113) obtained by encrypting a previously given content decryption key using said at least one node encryption key in the selected node encryption key group; a content receiving unit operable to receive a content via the network; an encryption unit (114) operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key; and a transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the content output apparatuses.

It should be noticed that the content encryption key is identical to the content decryption key since D1 mentions the Data Encryption Standard, see par. 0070. Furthermore each apparatus 1..16 is previously assigned a key IK1...IK16 and the node encryption keys are selected as a function of the invalidated reproducing device, see par. 108-109 and 112. As a consequence the subject-matter of claim 1 lacks novelty.
A similar reasoning applies mutatis mutandis to the corresponding method claim 34 which therefore lacks novelty as well.

The additional features of dependent claim 2 i.e. the selection of a terminal node key and a key which is not a terminal node key is also known from D1, see passages mentioned above.

The additional features of dependent claim 3 are also known from D1.
The features mentioned in dependent claims 4-7, 9 and 10 represent merely several straightforward possibilities from which the skilled person would select, in accordance with circumstances, without the exercise of inventive skill, in order to solve the problem posed. The claims 4-7 and 10 therefore lack an inventive step as defined by Art. 33(3) PCT.

The subject-matter of independent claim 11 corresponds largely to claim 2 which therefore lacks novelty. The additional features of claims 14-16 are known from D1 whereas the features of claims 12 and 13 deal with obvious design measures the skilled person would adopt according to circumstances.

Claim 17 lacks novelty over D1 taking into account that the second receiving unit (1221) receives the selected key list. A similar reasoning applies mutatis mutandis to the corresponding method claim 35 which therefore lacks novelty as well. Dependent claims 18-20 represent obvious design measures.

Claim 21 lacks novelty over D1 taking into account that the technical features of the claim are explicitly or implicitly implied by the key management device (1201) which combines the function of an encrypted content server and a key issuing center.
A similar reasoning applies mutatis mutandis to the corresponding method claim 36 which therefore lacks novelty as well.
The additional features of dependent claim 23 are known from D1, whereas the additional

features of claims 22, 24-26 represent obvious design measures.

Claim 27 defines a content distribution system basically combining a content output apparatus according to claim 17 and a content distribution server according to claim 1. This combination is disclosed by D1. As a consequence the subject-matter of claim 27 is not novel.

Dependent claim 28 further combines the system of claim 27 with a key issuing center according to claim 21. This combination as well is disclosed explicitly or implicitly by D1. As a consequence the subject-matter of claim 28 is not novel.

Claim 29-33 address programs to be used by a content distribution server, a content output apparatus, a key issuing center and a key assignment method or a computer readable recording medium for recording such a program. It is obvious that the systems to which the claims relate may be implemented by a program. As a consequence claims 29-33 lack an inventive step.

The combination of the features of dependent claim 8 is neither known from, nor rendered obvious by, the available prior art since it increases the security and simplifies the key selection method of the prior art.